REMARKS

This Amendment responds to the Final Office Action dated January 29, 2007. Reconsideration is respectfully requested in view of these Remarks. The claims have not been amended herewith.

A) File History

In response to the prior Final Office Action, dated August 25, 2005, applicants filed an appeal and in response thereto all of the prior final rejections were withdrawn. Prosecution was subsequently re-opened and the claims were then rejected over US 5,956,404 to Schneier in an Office Action dated June 30, 2006. An interview was conducted between the Examiner and the undersigned representative on September 12, 2006, and subsequently the language of claims, 1, 16 and 31 was amended to clarify the relationship between the use of the ephemeral key pair in the encrypting and generating steps of the public-key message generation process. This second Final Office Action followed.

B) Rejection Under 35 U.S.C. § 112

The present Office Action concedes that the two part use of an ephemeral key pair in a single message generation process is not disclosed in Schneier, but now raises enablement and indefiniteness issues under 35 U.S.C. § 112 with respect to the independent claims. These rejections are traversed for the following reasons: (1) the use of the term "ephemeral key pair" in the claims is entirely consistent with the common usage of that term in the encryption field, contrary to the assertions in the Office Action; and (2) the application, as filed, contains sufficient information regarding the claimed subject matter to enable the person of skill in the art to make and use the claimed invention.

The indefiniteness rejection under 35 U.S.C. § 112, second paragraph, relies upon a faulty assumption – that the inventor's of this application are acting as their own lexicographers and are using the term "ephemeral key pair" in a manner that is contrary to its ordinary and customary meaning in the field. This is not the case. In fact, the use of the phrase "ephemeral key pair" in the present application is entirely consistent with the materials referred to in the Office Action in support of this faulty assumption and is also consistent with other materials supplied herewith at Tabs A and B.

In "Code & Cipher, Certicom's Bulletin of Security and Cryptography," Volume 1, Number 2, 2003, which is relied upon in the Office Action, it is stated that "An entity's ephemeral key pair is intended for exactly one use. The keys are created, used once in the calculation of a key establishment primitive and then destroyed immediately after the shared secret is computed." In addition, this article states that the primitive is a cryptographic building block that is used to "facilitate the implementation of more complicated schemes." The computation of the cryptographic primitive may then be used, for example, to enable secure two-party communications (where each party is generating their own ephemeral key pair) or one-party communications such as e-mail messages, where only the sender is generating the ephemeral key pair.

The usage of the phrase "ephemeral key pair" in the Code & Cipher reference is entirely consistent with the present application. In the invention described and claimed in this herein, a single ephemeral key pair is generated and used for a single message transaction between entities. As noted in the Background section of the application, there are three major processes in the public-key environment: (i) certification; (ii) encryption; and (iii) digital signature. Each time a message is sent via the public-key system, each of these processes may occur. In the

present invention, the ephemeral key pair that is generated in the encryption phase of the process of generating a secure message is also used in the digital signature phase of signing the secure message. The key pair is still "ephemeral," however, because a new ephemeral key pair will be generated for each message transaction. Thus, the key pair is used "only once" for each message transaction.

This one-time ephemeral key process is clearly shown in relation to FIG. 4 of the present application, which describes a process whereby Alice wants to send a secure message to Bob. In the certification stage of the process, Alice and Bob generate long term (*i.e.*, static) private keys which are used to compute public keys that are shared through a certification authority or through a public key repository. In the encryption phase of the process Alice generates an ephemeral key pair which is used to encrypt the message to be sent to Bob. Finally, in the digital signature phase of the process the ephemeral key pair from the encryption phase is used to generate the digital signature. As stated succinctly in the application, "The improved digital signature scheme of the present invention uses the encryption ephemeral key pair (X,x) produced in the encryption stage 50' as a substitute for the signature ephemeral key pair (Z,z) required in the digital stage 70'." Thus, in this manner, the ephemeral key pair is used only once for each message transaction, although in the present invention the ephemeral key pair is used for two distinct stages or phases of the secure message generation process. This is not inconsistent with the Code & Cipher articles' use of this same terminology.

This same reasoning applies to the other two references relied on in the Office Action, both of which are discussing one-time use of "ephemeral keys" in terms of a secure message transactions or processes, of which the encryption and digital signature phases may form a part. Further evidence of this correct interpretation of "ephemeral key pair" is found in the online

Wikipedia definition of the term as "A cryptographic key is called ephemeral if it is generated for each execution of a key establishment process," (Tab A, hereto) and also in "Cryptography and Network Security, Principles and Practice," 3rd Edition, by William Stallings, which states that Ephemeral Diffie-Hellman is a technique used to create "ephemeral (temporary, one time) secret keys." (Tab B, hereto) Again, in the present invention, the "ephemeral key pair" is used in a single secure message generation process that includes encryption and digital signature sub-steps, and thus is consistent with the ordinary and customary usage of the term by the person of skill in the art.

Regarding the enablement rejection, FIG. 4 of the present application, and its associated textual description, provides ample and complete information for the person of skill in the art to practice the claimed invention. These materials clearly show the public-key encryption process of a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair that is used to encrypt the plaintext message (16, 18, 20, 22 in FIG. 4); and b) generating a digital signature for the ciphertext message using the ephemeral key pair produced in the encrypting step (28', 32, 34' 36' in FIG. 4). The person of skill in the art, upon reviewing these materials, would know how to practice the claimed invention, and thus the specification is enabling under 35 U.S.C. § 112.

This application is in condition for allowance.

Respectfully submitted:

JONES DAY
David B. Cochran
Reg. No. 39,142
901 Lakeside Ave.
Cleveland Ohio, 44114
216-586-7029
dcochran@jonesday.com